[10191/3602]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES

Inventors	:	Jochen WEBER et al.
Serial No.	:	10/801,363
Filed	:	March 15, 2004
For	:	MICROPROCESSOR SYSTEM AND METHOD FOR DETECTING THE EXCHANGE OF MODULES OF THE SYSTEM
Examiner	:	Fatoumata TRAORE
Art Unit	:	2436
Confirmation No.	:	3174

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on:

Date: April 15, 2010 Reg. No. 36,197

Signature: _____
Jong H. Lee

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPELLANTS' APPEAL BRIEF
UNDER 37 C.F.R. § 41.37

S I R :

Applicants electronically filed a Notice of Appeal dated December 15, 2009, appealing from the Final Office Action dated June 15, 2009, in which claims 1-8, 10-16 and 18-24 of the above-identified application were finally rejected. This Appeal Brief is being submitted by Applicants in support of their appeal.

04/19/2010 SDENBOB3 00000020 110600 10801363
02 FC:1402 540.00 DA

I. REAL PARTY IN INTEREST

The real party in interest in the present appeal is Robert Bosch GmbH of Stuttgart, Germany. Robert Bosch GmbH is the assignee of the entire right, title, and interest in the present application.

II. RELATED APPEALS AND INTERFERENCES

No appeal or interference which will directly affect, or be directly affected by, or have a bearing on, the Board's decision in the pending appeal is known to exist to the undersigned attorney or is believed by the undersigned attorney to be known to exist to Applicants.

III. STATUS OF CLAIMS

Claims 1-8, 10-16 and 18-24 are currently pending in the present application. Claims 9 and 17 have been canceled. Claims 1-8, 10-16 and 18-24 are rejected and are being appealed. Among the appealed claims, claims 1, 10 and 23 are independent; claims 2-8 and 20-22 depend on claim 1; claims 11-16 and 18-19 depend on claim 10; and claim 24 depends on claim 23.

IV. STATUS OF AMENDMENTS

No Amendment has been made subsequent to the final Rejection mailed on June 15, 2009.

V. SUMMARY OF CLAIMED SUBJECT MATTER

With respect to independent claim 1, the present invention provides a microprocessor system including:

a plurality of modules including a microprocessor (Fig. 1, element 2) and at least one storage module (Fig. 1, element 3, memory location 6) for storing code and data for the microprocessor, at least one of the modules (Fig. 1, element 3, memory location 7) storing a serial number of the at least one module in a non-exchangeable manner; (Specification, p. 1, l. 29 – p. 2, l. 3; p. 4, l. 23 – p. 5, l. 9);

an arrangement for storing a code number (Fig. 1, memory location 6), the code number being obtained as a function of the serial number by using an encryption method, and for storing information required to calculate the serial number from the code number, (p. 2, l. 9-15 & 26-28; p. 5, l. 5-9);

wherein the microprocessor (Fig. 1, element 2) is adapted to calculate a serial number from the code number on the basis of the information, to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison; (p. 2, l. 9-19; p. 5, l. 5-20); and

wherein at least two of the modules are each identified by a serial number, and the code number is obtained by encrypting a linking of the serial numbers of the at least two of the modules (p. 7, l. 1-3).

With respect to independent claim 10, the present invention provides a method for detecting an exchange of a module, identified by a serial number, in a microprocessor system, the method including:

storing, in the microprocessor system, a code number, which is obtained from the serial number by using an encryption method, and storing information required for calculating the serial number from the code number; (p. 2, l. 9-15 & 26-28; p. 5, l. 5-9);

reading the code number and calculating an unencrypted serial number as a function of the code number with the aid of the information; (p. 2, l. 9-15; p. 5, l. 5-10; p. 6, l. 4-6);

comparing the decrypted serial number thus obtained with the serial number of the module; (p. 5, l. 10-12); and

detecting an exchange of the module if the serial number of the module does not match the decrypted serial number, (p. 5, l. 10-13);

wherein the method is used for a plurality of modules of the microprocessor system, and the code number is obtained by encrypting a linking of the serial numbers of the plurality of modules (p. 7, l. 1-3).

With respect to independent claim 23, the present invention provides a microprocessor system including:

a plurality of modules including a microprocessor (Fig. 1, element 2) and at least one storage module (Fig. 1, element 3, memory location 6) for storing code and data for the microprocessor, at least one of the modules (Fig. 1, element 3, memory location 7) storing a serial number of the at least one module in a non-exchangeable manner; (Specification, p. 1, l. 29 – p. 2, l. 3; p. 4, l. 23 – p. 5, l. 9);

an arrangement for storing a code number (Fig. 1, memory location 6), the code number being obtained as a function of the serial number by using an encryption method, and for storing information required to calculate the serial number from the code number, (p. 2, l. 9-15 & 26-28; p. 5, l. 5-9);

wherein the microprocessor (Fig. 1, element 2) is adapted to calculate a serial number from the code number on the basis of the information, to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison, (p. 2, l. 9-19; p. 5, l. 5-20), and wherein the information required to calculate the serial number from the code number is stored in a different storage module (Fig. 2, element 11) than the code number (Fig. 2, element 3), the different storage module being connected to the microprocessor in a non-separable manner (p. 3, l. 17-32; p. 5, l. 30 – p. 6, l. 11).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following grounds of rejection are presented for review on appeal in this case:

(A) Whether pending claims 1, 3, 10-12, 20 and 21 are unpatentable under 35 U.S.C. § 103(a) as obvious over U.S. Patent No. 7,308,718 ("Brookner") in view of U.S. Patent No. 6,792,113 ("Ansell").

(B) Whether pending claims 4, 5, 13, 14, 23 and 24 are unpatentable under 35 U.S.C. § 103(a) as obvious over Brookner in view of Ansell and U.S. Patent No. 5,771,287 ("Gilley").

(C) Whether pending claims 6-8, 15 and 16 are unpatentable under 35 U.S.C. § 103(a) as obvious over Brookner in view of Ansell and U.S. Patent No. 5,774,544 ("Lee").

(D) Whether pending claims 18, 19 and 22 are unpatentable under 35 U.S.C. § 103(a) as obvious over Brookner in view of Ansell and U.S. Patent No. 6,026,293 ("Osborn").

VII. ARGUMENTS

A. Rejection of Claims 1-3, 10-12, 20 and 21

Claims 1-3, 10-12, 20 and 21 were rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 7,308,718 ("Brookner") in view of U.S. Patent No. 6,792,113 ("Ansell"). Applicants respectfully submit that the rejections should be withdrawn for at least the following reasons.

In rejecting a claim under 35 U.S.C. § 103(a), the Examiner bears the initial burden of presenting a *prima facie* case of obviousness. In re Rijckaert, 9 F.3d 1531, 1532, 28 U.S.P.Q.2d 1955, 1956 (Fed. Cir. 1993). To establish a *prima facie* case of obviousness, the Examiner must show, *inter alia*, that there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify or combine the references, and that, when so modified or combined, the prior art teaches or suggests all of the claim limitations. M.P.E.P. §2143. In addition, as clearly indicated by the Supreme Court, it is "important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the [prior art] elements" in the manner claimed. See KSR Int'l Co. v. Teleflex, Inc., 82 U.S.P.Q.2d 1385 (2007). In this regard, the Supreme Court further noted that "rejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some

rational underpinning to support the legal conclusion of obviousness." Id., at 1396. To the extent that the Examiner may be relying on the doctrine of inherent disclosure in support of the obviousness rejection, the Examiner must provide a "basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristics necessarily flow from the teachings of the applied art." (See M.P.E.P. § 2112; emphasis in original; see also Ex parte Levy, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990)).

Claim 1 recites, in relevant parts, "a plurality of modules including a microprocessor and at least one storage module for storing code and data for the microprocessor, at least one of the modules storing a serial number of the at least one module in a non-exchangeable manner; **an arrangement for storing a code number, the code number being obtained as a function of the serial number by using an encryption method**, and for storing information required to calculate the serial number from the code number, . . . wherein **at least two of the modules are each identified by a serial number, and the code number is obtained by encrypting a linking of the serial numbers of the at least two of the modules**." Claim 10 recites substantially similar features as the above-recited features of claim 1.

In support of the rejection, the Examiner contends that column 6, lines 5-20 of the secondary Ansell reference discloses a **code number** obtained by **encrypting a linking of the serial numbers of at least two modules**. However, the cited section merely describes a hardware identifier 140 generated as a hash function of the serial numbers of various components of a single client system. As further described in the paragraph beginning on column 9, line 52, **the hardware identifier 140 is not itself encrypted**, but instead is used for encrypting and decrypting a private key. Thus, the hardware identifier 140 does not constitute an **encrypted linking** of serial numbers.

In the Advisory Action of August 17, 2009, the Examiner responds to the above argument of Applicants by contending that "the hardware identifier is a hash of serial number of processor, MAC address of network card and/or serial number of one or more hard disc drive," and that "hashing is the same as encrypting, since they both [involve] a step of transforming data/information to make it unreadable." However, the Examiner's contention that "hashing is the same as encrypting" is both factually and legally incorrect, as explained in detail below.

The fundamental rule of claim interpretation is the claim must be given the broadest reasonable interpretation that is consistent with the specification and the interpretation that those skilled in the art would reach (MPEP 2111, citing Phillips v. AWH Corp., 75 U.S.P.Q.2d 1321 (Fed. Cir. 2005), and In re Cortright, 49 U.S.P.Q.2d 1464, 1468 (Fed. Cir. 1999)). Applying this interpretation rule the present claimed limitation "**the code number being obtained as a function of the serial number by using an encryption method**, . . . wherein . . . **the code number is obtained by encrypting a linking of the serial numbers of the at least two of the modules**," there is no reasonable basis for the Examiner contention that the "encryption" limitation is met by the hashing discussion in Ansell. First, one of ordinary skill in the art would readily understand that "encryption" and "hashing" are completely different concepts: "encryption" involves transformation of information using a key, while "hashing" does not involve the use of a key. This understanding is entirely consistent with the disclosure of the present application which specifically discloses the use of keys for encryption and decryption: "The encryption method by which the code number is obtained from the serial number is preferably an asymmetrical method, i.e., a method that uses different keys for encryption and decryption." (Specification, p. 2, l. 26-28). As clearly described in column 9, l. 56 – col. 10, l. 3 of Ansell, the hardware identifier 140 is the **key** used for encrypting and decrypting the private key 2404, but **the hardware identifier 140 itself is not obtained "using an encryption method**," let alone "**obtained by encrypting a linking of the serial numbers of the at least two of the modules**."

Independent of the above, to the extent the Examiner contends in the Final Office Action that the encrypted serial number disclosed in the primary Brookner reference meets the "code number" limitations of claim 1, this contention is factually incorrect. Brookner describes a process involving encrypting a serial number of a processor-controlled system, transmitting the encrypted serial number from the system to a server, decrypting the encrypted serial number using a public key, and comparing the decrypted serial number to a serial number stored in a record on the server. Although Brookner mentions that the serial number is pre-stored, the subsequently **encrypted** serial number is merely transmitted, not stored. With respect to the **stored values in Brookner**, e.g., the public key and the stored serial number, **none of these stored values are generated as a function of encrypting the system's serial number**. Thus, Brookner simply does not teach or suggest the present claimed limitation of "**an arrangement for storing a code number**, **the code number being obtained as a function of the serial number by using an encryption method**," as recited in claim 1. In

addition, Ansell similarly fails to teach or suggest this limitation of claim 1. Thus, the overall teachings of Brookner and Ansell cannot suggest "**an arrangement for storing a code number, the code number being obtained as a function of the serial number by using an encryption method**."

For at least the foregoing reasons, claims 1 and 10, as well as dependent claims 2, 3, 11, 12, 20 and 21, are not rendered unpatentable by the combination of Brookner and Ansell. Reversal of the obviousness rejection of claims 1-3, 10-12, 20 and 21 is respectfully requested.

B. Rejection of Claims 4, 5, 13, 14, 23 and 24

Claims 4, 5, 13, 14, 23 and 24 were rejected under 35 U.S.C. § 103(a) as unpatentable over Brookner in view of Ansell and U.S. Patent No. 5,771,287 ("Gilley").

Claims 4 and 5 ultimately depend on claim 1, and claims 13 and 14 ultimately depend on claim 10. Independent claim 23 recites limitations substantially similar to the limitations of claims 1 and 10 discussed above, i.e., claim 23 recites, in relevant parts, "**an arrangement for storing a code number, the code number being obtained as a function of the serial number by using an encryption method**." As noted above, Brookner and Ansell fail to teach or suggest the present claimed limitation "**an arrangement for storing a code number, the code number being obtained as a function of the serial number by using an encryption method**," as recited in claims 1 and 23 (and as similarly recited in parent claim 10). Furthermore, the secondary Gilley reference similarly fails to teach or suggest the above limitation, and therefore does not cure the critical deficiencies of Brookner and Ansell as applied against parent claims 1, 10 and 23. Accordingly, dependent claims 4, 5, 13 and 14, as well as independent claim 23 and its dependent claim 24, are not rendered obvious by Brookner, Ansell and Gilley.

For at least the foregoing reasons, reversal of the obviousness rejection of claims 4, 5, 13, 14, 23 and 24 is requested.

C. Rejection of Claims 6-8, 15 and 16

Claims 6-8, 15 and 16 were rejected under 35 U.S.C. § 103(a) as unpatentable over Brookner in view of Ansell and U.S. Patent No. 5,774,544 ("Lee").

Claims 6-8 ultimately depend on claim 1, and claims 15-16 ultimately depend on claim 10. As noted above, Brookner and Ansell fail to teach or suggest the present claimed limitation "**an arrangement for storing a code number, the code number being obtained as a function of the serial number by using an encryption method**," as recited in parent claim 1 (and as similarly recited in parent claim 10). Furthermore, the secondary Lee reference similarly fails to teach or suggest the above limitation, and therefore fails to cure the critical deficiencies of Brookner and Ansell as applied against parent claims 1 and 10. Accordingly, dependent claims 6-8 and 15-16 are not rendered obvious by Brookner, Ansell and Lee.

For at least the foregoing reasons, reversal of the obviousness rejection of claims 6-8 and 15-16 is requested.

D. Rejection of Claims 18, 19 and 22

Claims 18, 19 and 22 were rejected under 35 U.S.C. § 103(a) as unpatentable over Brookner in view of Ansell and U.S. Patent No. 6,026,293 ("Osborn").

Claim 22 ultimately depends on claim 1, and claims 18 and 19 ultimately depend on claim 10. As noted above, Brookner and Ansell fail to teach or suggest the present claimed limitation "**an arrangement for storing a code number, the code number being obtained as a function of the serial number by using an encryption method**," as recited in parent claim 1 (and as similarly recited in parent claim 10). Furthermore, the secondary Osborn reference similarly fails to teach or suggest the above limitation, and therefore fails to cure the critical deficiencies of Brookner and Ansell as applied against parent claims 1 and 10. Accordingly, dependent claims 18, 19 and 22 are not rendered obvious by Brookner, Ansell and Osborn.

For at least the foregoing reasons, reversal of the obviousness rejection of claims 18, 19 and 22 is requested.

VIII. CONCLUSION

For the foregoing reasons, it is respectfully submitted that the final rejections of claims 1-8, 10-16 and 18-24 should be reversed.

Claims Appendix, Evidence Appendix and Related Proceedings Appendix sections are found in the attached pages.

Respectfully submitted,

KENYON & KENYON LLP

(R. No. 36,197)

Dated: April 15, 2010

By: JONG LEE for Gerard Messina

Gerard A. Messina
Reg. No. 35,952
One Broadway
New York, New York 10004
(212) 425-7200

APPENDIX TO APPELLANTS' APPEAL BRIEF UNDER 37 C.F.R. § 41.37

CLAIMS APPENDIX

The claims involved in this appeal, claims 1-8, 10-16 and 18-24, in their current form after entry of all amendments presented during the course of prosecution, are set forth below:

1. A microprocessor system comprising:

a plurality of modules including a microprocessor and at least one storage module for storing code and data for the microprocessor, at least one of the modules storing a serial number of the at least one module in a non-exchangeable manner;

an arrangement for storing a code number, the code number being obtained as a function of the serial number by using an encryption method, and for storing information required to calculate the serial number from the code number,

wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information, to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison; and

wherein at least two of the modules are each identified by a serial number, and the code number is obtained by encrypting a linking of the serial numbers of the at least two of the modules.

2. The microprocessor system according to claim 1, wherein the encryption method is asymmetrical, the code number is calculated from the serial number with the aid of a secret key, and the information includes a public key as well as a program code for calculating the serial number from the code number.

3. The microprocessor system according to claim 2, wherein one of the at least one module identified by the serial number is a storage module.

4. The microprocessor system according to claim 3, wherein the code number is stored in a same storage module as the serial number.

5. The microprocessor system according to claim 3, wherein the storage module is an electrically rewritable, non-volatile memory, and the code to be executed if the calculated and the stored serial numbers do not match includes a command for deletion of the storage module.

6. The microprocessor system according to claim 1, wherein one of the at least one module identified by the serial number is the microprocessor.

7. The microprocessor system according to claim 1, wherein the information required to calculate the serial number from the code number is stored in a different storage module than the code number.

8. The microprocessor system according to claim 7, wherein the different storage module is connected to the microprocessor in a non-separable manner.

10. A method for detecting an exchange of a module, identified by a serial number, in a microprocessor system, the method comprising:

storing, in the microprocessor system, a code number, which is obtained from the serial number by using an encryption method, and storing information required for calculating the serial number from the code number;

reading the code number and calculating an unencrypted serial number as a function of the code number with the aid of the information;

comparing the decrypted serial number thus obtained with the serial number of the module; and

detecting an exchange of the module if the serial number of the module does not match the decrypted serial number,

wherein the method is used for a plurality of modules of the microprocessor system, and the code number is obtained by encrypting a linking of the serial numbers of the plurality of modules.

11. The method according to claim 10, wherein an asymmetric encryption method is used and a public key of the encryption method is included in the information required to calculate the serial number from the code number.

12. The method according to claim 10, wherein the module is a storage module of the microprocessor system.

13. The method according to claim 12, wherein the code number is stored in the same storage module as the serial number.

14. The method according to claim 12, further comprising deleting a content of the storage module if an exchange of the module has been detected.

15. The method according to claim 10, wherein the module includes a microprocessor of the microprocessor system.

16. The method according to claim 10, wherein at least the information required for calculating the serial number is stored in a different storage module than the code number.

18. The method according to claim 10, wherein steps of the method are executed upon each start-up of the microprocessor system.

19. The method according to claim 10, wherein steps of the method are periodically executed during operation of the microprocessor system.

20. The microprocessor system according to claim 1, wherein each of the modules is identified by a serial number, and the code number is obtained by encrypting a linking of the serial number of the each of the modules.

21. The microprocessor system according to claim 1, wherein the microprocessor is adapted to calculate a linking of the serial numbers of the at least two modules from the code number on the basis of the information, to compare the calculated serial number to the stored linking of the serial numbers of the at least two modules.

22. The microprocessor system according to claim 1, wherein the microprocessor is adapted to calculate the serial number from the code number at regular time intervals during operation.

23. A microprocessor system, comprising:

a plurality of modules including a microprocessor and at least one storage module for storing code and data for the microprocessor, at least one of the modules storing a serial number of the at least one module in a non-exchangeable manner;

an arrangement for storing a code number, the code number being obtained as a function of the serial number by using an encryption method, and for storing information required to calculate the serial number from the code number,

wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information, to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison, and wherein the information required to calculate the serial number from the

code number is stored in a different storage module than the code number, the different storage module being connected to the microprocessor in a non-separable manner.

24. The microprocessor according to claim 23, wherein the different storage module and the microprocessor are integrated in a one-chip microprocessor.

EVIDENCE APPENDIX

In the present application, there has been no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131 or 1.132, or other evidence entered by the Examiner and relied upon by Appellant in the present appeal.

RELATED PROCEEDINGS APPENDIX

No appeal or interference which will directly affect, or be directly affected by, or have a bearing on, the Board's decision in the pending appeal is known to exist.